January 26, 2024

Overall rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple vulnerabilities in the J-Web component of Juniper Networks Junos OS on SRX Series and EX Series. These issues affect all versions of Juniper Networks Junos OS on SRX Series and EX Series.

Technical Details

An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J-Web of Juniper Networks Junos OS on SRX Series and EX Series allows an attacker to construct a URL that when visited by another user enables the attacker to execute commands with the target's permissions, including an administrator. A specific invocation of the emit_debug_note method in webauth_operation.php will echo back the data it receives.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: Required

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-21619, CVE-2023-36846, CVE-2024-21620, CVE-2023-36851
- 2024-01 Out-of-Cycle Security Bulletin: Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web have been addressed
- VRM Vulnerability Reports